UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/447,312	11/22/1999	SCOTT D. BLANCHARD	IRI03844	3661

22863 7590 03/24/2005

MOTOROLA, INC.
CORPORATE LAW DEPARTMENT - #56-238
3102 NORTH 56TH STREET
PHOENIX, AZ 85018

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/447,312	BLANCHARD ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

Response to Arguments

2. In view of Applicant's arguments filed 10/26/2004 a new ground (s) of rejection is presented in this office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1-4, 17-19 and 223 are** rejected under 35 U.S.C. 102(b) as being anticipated by US patent 5,862,160 to Irvin et al. (hereinafter "Irvin").

As per claims 1, Irvin teaches a method of adding packet ordering information to a plurality of data packets [abstract, col. 3, lines 27-49] comprising:

applying error detection codes to each of the plurality of data packets [col. 4, lines 62-67, col. 8, lines 36-43];

and masking each of the plurality of data packets to which the error detection codes have been applied [col. 5, lines 2-11, i.e. a mask selector is selecting a mask, or data bit pattern and combines the selected mask and the encoded input signal to form a combined (col. 6, lines 19-22)] ,

Irvin discloses one mask for every specified piece of information [col. 9, lines 19-27, i.e. see also col. 5, lines 54-59, col. 6, lines 1-5, col. 5, lines 2-11, i.e. a mask selector is selecting a mask, or data bit pattern],

Irvin teaches the masking being performed using a plurality of ordering masks in a known order [col. 5, lines 2-4, col. 6, lines 18].

As per claim 2, Irvin teaches the method of claim 1 wherein masking comprises exclusive or'ing each of the plurality of data packets with a corresponding one of the plurality of ordering masks [col. 3, lines 39-48, col. 7, lines 25-54].

As per claim 3, Irvin teaches the method of claim 1 wherein each of the plurality of data packets to which the error detection codes have been applied is masked with one of the plurality of ordering masks [col.7, lines 16-23, i.e. one mask for each possible data state received over the line 224] , the plurality of ordering masks and the known order being known by a receiver such that the receiver can discern a relative packet order using the plurality of ordering masks [col. 3, lines 44-48].

As per claim 4, Irvin teaches the method of claim 1, wherein the plurality of ordering masks comprises cryptographic keys [col. 4, lines 12-28, i.e. XORing a data frame with a mask represents encryption where the mask is cryptographic key].

As per claim 16, Irvin teaches a packet receiver (see Fig. 3, col. 6, lines 22-23, demodulator receives and demodulate the signal transmitted), a mask store (col. 3, lines 66-67, col. 4, lines 4-11), an unmasking device coupled to the mask store (col. 7, line 61 through col. 8, line 4, exclusive XOR circuit) and the packet receiver, the unmasking device being configured to unmask received packets; and an error detection device [see also col. 4, lines 4-11, i.e. logic

device is for combining a select mask] coupled to the unmasking device, the error detection device being configured to detect errors in unmasked received packets [logic device performs CRC error checking].

As per claim 17, Irvine teaches the communications device of claim 16 further comprising a controller coupled to the mask store and the error detection device [col. 7, line 57-61, i.e. a CPU is connected to excusive OR circuit and to the logic device. CPU transmits and receives frames to exclusive or and control signals to logic device], the controller [logic device] being configured to evaluate error information received from the error detection device [col. 8, lines 33-52], and further configured to command the mask store to provide masks to the unmasking device [col. 7, lines 61-62].

As per claim 18, Irvin teaches the communications device of claim 17 wherein the mask store includes a plurality of masks, the plurality of masks representing an order of transmission of a plurality of packets [col. 4, line 66 through col. 4, line 1, i.e. the store includes at least one data mask to represent at least one possible input data bit pattern, see also col. 6, lines 1-11].

As per claim 19, Irvin teaches the mask is a key generator capable of generating keys to decrypt encrypted packets [col. 6, lines 43-64, i.e. the error protection decoder (containing the mask store) logically combines each mask stored in the receiving system with the received signal by XoRing)].

As per claim 23, Irvin teaches a packet formatted adapted to receive data packets and configured to supply formatted packets (col. 5, lines 36-39, i.e. source encoder 104, encodes input signal 108 to convert input signal into a form suitable for transmission), a forward error device coupled to receive the formatted packets from the packet formatter and configured to

apply error codes (col. 5, lines 39-49, i.e. error protection encoder 112 produces parity bits according to a CRC code). Irvin encoded signals have appended error detection bits. Irvine teaches a mask store (col. 5, lines 50-54). Irvine teaches a masking device to mask each of the formatted packets to which the error codes have been applied (col. 5, lines 1-11, i.e. logic circuit 124 for logically combining the mask produced by mask selector 120 with the encoded signal 112).

4. **Claims 1-6, 16-19, 23-26** rejected under 35 U.S.C. 102(b) as being anticipated by prior art of record, Hosford et al, hereinafter Hosford (USP 5,966,450).

As per claim 1, Hosford teaches applying error detection codes to each of the plurality of data packets (frames, see column 1, lines 19-23). Hosford teaches masking each data packet with masks (variable masks, see column 1, line 66--column 2, line 2). Hosford teaches that each mask differs and the order that they were created is maintained through a variable value such as a frame counter to preserve order (column 2, lines 11-15).

As per claim 2, Hosford teaches applying the mask to the data packets using XoRing (column 2, lines 910).

As per claim 3, Hosford teaches each of the data packets (frames) are masked with one of the ordering masks (column 1, lines 66-67).

As per claim 4, Hosford teaches the masks comprise randomly generated numbers (column 2, lines 49). A key is equivalent to a random number.

As per claim 6, Hosford teaches his system is implemented on a TDMA protocol (column 1, lines 15) and can be also used on wireline communication systems (column 6, lines 25-27). TDMA has a maximum latency variability. It is inherent that Hosford's systems will

therefore have a sufficient number of masks so that the receiver can discern the proper order of the packets.

As per claim 16, Hosford teaches a packet receiver (column 3, line 10), a mask store (column 2, line 65-column 3, line 2), an unmasking device coupled to the mask store (column 3, lines 60-65). A mask store is taught by the fact that the sender generates a different mask for each data frame. An unmasking device is necessarily coupled to the sender and receiver because it is inherent that data can flow both ways. Therefore, both stations have the necessary resources to send and receive data masked data packets. Hosford teaches that data packets have error detection bits added (column 1, lines 20-23). Knowing this, the receiver inherently checks these error bits once the data packet is decrypted.

As per claim 17, Hosford teaches adding error detection codes data packets so it is inherent that the device can evaluate errors and take the appropriate action. A controller is taught Hosford where he describes both stations having a processor (column 3, line 25). Hosford teaches the masks must again be used to unmask the data packets (column 3, lines 10-14). This would require the unmasking device being coupled to the mask store.

As per claim 18, Hosford teaches the masks represent an order of transmission of a plurality of packets (column 2, lines 12-13). Hosford teaches a frame counter is part of the mask and is incremented after each frame.

As per claim 19, Hosford teaches the mask is a key generator capable of generating keys to decrypt encrypted packets (column 2, lines 3-8 and column 3, lines 10-13).

As per claim 23, Hosford teaches a packet formatted adapted to receive data packets and configured to supply formatted packets (column 1, lines 16-20), a forward error device coupled

to receive the formatted packets from the packet formatter and configured to apply error codes (column 1, lines 19-23). Hosford teaches digitized speech frames have appended error detection bits. Hosford teaches a mask store (column 2, line 65-column 3, line 2). Hosford teaches a masking device to mask each of the formatted packets to which the error codes have been applied (column 2, lines 415).

As per claim 24, Hosford teaches a data packet formatter (column 1, lines 1617).

As per claim 25, Hosford teaches the packet formatter comprises a vocoder (digitized speech frames, see column 1, line 19).

As per claim 26, Hosford teaches the masking device comprises an encryptor by teaching that the masking device performs encryption from randomly generated numbers (keys), see column 2, lines 4-9.

Claim Rejections - 35 USC ' 103

5. **Claims 5 and 27** are rejected under 35 U.S.C. 103(x) as being unpatentable over Hosford in view of Weiss (USP 4,754,482).

As per claims 5 and 27, Hosford teaches the masks can be created from a cellular authentication voice privacy and encryption algorithm (column 2, lines 54-59). Hosford is silent in disclosing the encrypting of data packets prior to applying error detection. Weiss teach appending error detection codes to encrypted data packets (column 5, lines 2-9). The error detection codes would alert the receiver if the encrypted packet experienced a transmission error. It would be advantageous to know if a transmitted packet had any errors in it. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ

the teachings of Weiss within the system of Hosford because it would allow detection of errors in transmitted encrypted data packets.

6. **Claims 7-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss in view of Hosford in view of Gross (USP 5,761,431).

As per claim 7, Weiss teaches a method of determining a packet order of a received packet comprising: applying at least one ordering mask to the received packet from a list of ordering masks to find a current ordering mask that was previously used to mask the received packet (column 6, lines 23-29). Weiss is silent in disclosing that the sequence numbers correspond to a list of masks having a known order. Hosford teaches that a unique mask is generated for each frame of data and generated masks are kept in order by a frame counter (see column 1, line 66-column 2, line 2). The frame counter is used to create the mask (column 2, lines 11-12). Using a frame counter to unique identify each mask frame provides a way in which the receiver can find the current mask. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Hosford within the system of Weiss because using a relationship between the mask and the sequence number will allow the receiver can discern which packets have not arrived and allow the receiver to determine the correct packet order.

Weiss is silent in disclosing to delete older sequence numbers (masks). Gross et al teaches to remove stale data packets as they reach the top of a FIFO buffer (column 14, line 14). Discarding old data packets is necessary for receiver to remain ready to process the incoming data. In view of this, it would have been obvious to one or ordinary skill in the art at the time of

the invention to employ the teachings of Gross et al within the system of Weiss because it would allow one to remove older packets (after determining with masks) from the list (buffer).

As per claim 8, Weiss teaches checking the incoming packet with a synchronous sequence number, checking for errors, and updating sequence numbers when no errors are found (column 6, lines 23-39).

As per claim 9, Weiss teaches to check the errors by comparing the calculated error code with an error code that the receiver calculates (column 6, line 30-35).

As per claim 10, Weiss teaches applying stored sets of CRC's to determine if the correct packet has been received. Preservation of order is being maintained (column 12, lines 49-65). The CRC's in the list would then correspond to a particular sequence number (mask) (column 14, line 14). Weiss also teaches that if a packet is received in error that the receiving process can continue without losing synchronization. This implies that the erroneous packet is discarded (column 14, line 48).

7. **Claims 11-12 and 14-15** are rejected under 35 U.S.C. 103(x) as being unpatentable over Weiss in view of Dent et al, hereinafter Dent (USP 5,353,352).

As per claim 11, Weiss teaches a CRC list that is used to hold incoming data packets that are received out of order (column 12, lines 49-65). The CRC is computed from the sequence number of the receiver, which is synchronized to the transmitter (column 15, lines 15-25). These numbers are used to preserve the order of the received packets.

Weiss is silent in disclosing the use of ordering masks. Dent teaches the combining error codes with a mask (column 9, lines 12-14). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the

teachings of Dent within the Weiss because it would allow a two level ciphering system to improve the security of the system. The system of Weiss would still function as described now using the masks in place of just a CRC.

Weiss teaches the use of a buffer or list to hold these numbers as they are received. It is notoriously well known in the art how to search, traverse, add, and remove entries from buffers by setting pulling a data value from memory (temporarily) to compare it to another value. While the language in the claim is not exactly identical with the method described by Weiss to traverse a memory buffer, the outcome is the same. The lists of mask are each compared to a current received mask in order to determine which packet has been received and which order it belongs. Weiss also teaches to check the received packets for errors via the CRC (column 15, line 15).

As per claim 12, Examiner supplies the same rationale to combine Dent and Weiss, Dent's masks in the system of Weiss do maintain masks in a particular order. Weiss uses a sequence number which is correlated to the masks to preserve order.

As per claim 14, Weiss teaching of the use of sequence numbers in conjunction with the masks of Dent's system would determine that the lowest number received is the current order mask.

As per claim 15, Weiss is silent in disclosing the use of cryptographic keys in the masks. Dent teaches the use of cryptographic keys in the masks (column 23, lines 5560). Again this increases the security of the system be requiring a key to be used to unmask the packets. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Dent within the system of Weiss because it would only allow the rightful recipient to unmask the data.

8. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss and Dent as applied to claim 11 and in further view of Gross et al (USP 5,761,431).

As per claim 13, discarding the packet because a new packet is received is not explicitly taught by Weiss. Gross et al does refer to this occurrence as a stale packet and teaches to discard this packet (column 14, line 14). This would help the receiver and transmitter to remain synched with one another. It is also beneficial to drop late packets in some types of communication such as voice. In view of this, it would have been obvious to one of ordinary skill in the art to employ the teachings of Gross within the system of Weiss because it would allow one to discard packets, which are older than previously received packets.

Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hosford in view of Dent.

As per claim 20, Hosford is silent in teaching that the masks are buffered used more than once. Dent teaches reusing masks in a set more than once (column 20, lines 32-33). If masks are reused then they must be preserved in memory. It would be advantageous to reuse masks to reduce the computational time required to constant regenerate for every frame. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Dent within the system Hosford because it would allow the reuse of masks periodically instead of having to constantly compute new masks.

As per claim 21, Hosford explicitly teach the use of a pointer to keep track of the most recent mask pointer. Hosford does teach incrementing a frame counter. The frame counter essentially does the function of a pointer by indicating the last masked used because the frame counter is part of the mask. It would have been obvious to one or ordinary skill in the art at the

time of the invention to use the frame counter as a pointer to keep track of the most recently use masks because the sender and receiver must stay synchronized. Maintaining synchronization requires the order to be preserved and allows the receiver to know the next expected mask to be received.

9. **Claims 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Hosford.

As per claim 22, Hosford does not teach that a separation between the decryptor and the unmasking device. Hosford's unmasking device decrypts and unmasks because supplies generating a mask (unlocking key) from randomly generating bytes (column 3, lines 10-14). The unmasking mask is essentially the same as a key to undo the encryption. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of modify the teaching of Hosford to incorporate a separate decryptor because it does not change the overall function of Hosford's system. Functionally they are equivalent if unmasking comprises the function of decryption.

Conclusion

10. Prior arts made of record, not relied upon:

USP 6,141,788 is directed to a method for applying forward error correction in a transmission network includes the steps of choosing one of a plurality of possible error correction codes, using an appropriate field to encode a complete forward-error-correcting (FEC) code algorithm in each FEC packet to be transmitted. The packet stream, consisting of media packets and FEC packets can be sent to both FEC-capable and FEC-incapable receivers. Decoding methods are independent of the forward-error-correcting code transmitted. The sender can adapt the forward-error-correction code algorithm and the degree of error correction

provided on a one-time basis or even more dynamically. Decoding and recovery at the receiver require no prior notification from the sender. Applying the FEC code algorithm to decode includes interrogating the bits in an offset bit mask in each FEC packet to yield links with media packets, and applying other fields of the FEC header to obtain instructions to recover lost data in one of the media packets. Based thereon, reiterative decoding of media packets ensures that lost data recoverable with combinations of media packets and FEC packets are recovered.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. A.

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100